KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

Independent Accountant's Report

To the Management of Symantec Corporation:

We have examined for its certification authority (CA) operations at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan, Symantec's disclosure of its extended validation SSL ("EV SSL") certificate life cycle management business practices, including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the Symantec website, the provision of such services in accordance its disclosed practices, and the effectiveness of its controls over key and EV SSL certificate integrity, over the authenticity and confidentiality of EV SSL subscriber and relying party information, and over continuity of key and EV SSL certificate life cycle management operations, throughout the period December 1, 2015 to June 15, 2016 for the Symantec Trust Network (STN) CAs listed in Appendix A ("the STN Root and EV SSL Issuing CAs").

These disclosures and controls are the responsibility of Symantec's management. Our responsibility is to express an opinion on the conformity of these disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.4.5, based on our examination.

We conducted our examination in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of Symantec's EV SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
(2) selectively testing transactions executed in accordance with disclosed EV SSL certificate life cycle management practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at Symantec and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, Symantec's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

We noted the following matters that resulted in a modification of our opinion:

	Impacted WebTrust for CAs Criteria	Matters Noted
1	Verification of Applicant Principle 2, Criterion 13 requires that the CA maintains controls and procedures to provide reasonable assurance that for each Fully-Qualified Domain Name listed in a Certificate, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by only using at least one of the following verification methods: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; 2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; 4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at -sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; Verification of EV SSL Certificate requests Principle 2, Criterion 18 requires that, in cases where an EV SSL Certificate Request is submitted by a Certificate Requester, the CA maintains controls to provide reasonable assurance that, before it issues the requested EV SSL Certificate, it verifies that an authorized Certificate Approver reviewed and approved the EV SSL Certificate Request.	It was noted that Issuing EV SSL CAs were used to issue certificates for Symantec internal testing purposes for registered domains that Symantec did not own. As required by the CPS, Symantec did not obtain the required authorization from the respective registered domain owners prior to certificate issuance. Furthermore, certificates were also issued for internal testing purposes to unregistered domains. This caused WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL V 1.4.5 Principle 2, Criteria 13 and 18, to not be met.

Impacted WebTrust for CAs Criteria		Matters Noted
2	Principle 2, Criterion 49 requires that the CA and RA maintain controls to provide reasonable assurance that event logs at the CA and RA site are retained for at least seven years.	It was noted that physical access entry and exit logs for one of the CA facilities were not archived for 7 years as specified in the STN CPS. This caused WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL V 1.4.5 Principle 2, Criterion 49, to not be met with respect to the retention of CA facility entry and exit logs.

In our opinion, except for the effects of the matters discussed in the preceding paragraphs, in providing its STN EV SSL CA services in Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia, USA; Dublin Ireland; and Kawasaki-shi, Japan, during the period December 1, 2015 to June 15, 2016, in all material respects:

- Symantec disclosed its extended validation SSL ("EV SSL") certificate life cycle management business practices in its Symantec Trust Network Certification Practice Statement, Version 3.8.24 dated May 20, 2016 ("STN CPS"); and Symantec Trust Network Certificate Policy, Version 2.8.20, dated May 20, 2016 ("STN CP") including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the Symantec website, and provided such services in accordance with its disclosed practices

- Symantec maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their life cycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by Symantec)

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.4.5.

This report does not include any representation as to the quality of Symantec's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.4.5, nor the suitability of any of Symantec's services for any customer's intended purpose.

KPMG LLP

Certified Public Accountants
Santa Clara, CA
February 28, 2017

APPENDIX A –STN Root and EV SSL Issuing CAs

Symantec Root CAs:	**Symantec EV SSL Issuing CAs:**
• Symantec Class 3 Public Primary Certification Authority - G4 • VeriSign Class 3 Public Primary Certification Authority - G4 • VeriSign Class 3 Public Primary Certification Authority - G5 • Symantec Class 3 Public Primary Certification Authority - G6 • Symantec Class 3 Public Primary Certification Authority - G7 • VeriSign Universal Root Certification Authority	• VeriSign Class 3 Extended Validation SSL CA • VeriSign Class 3 Extended Validation SSL SGC CA • VeriSign Class 3 Extended Validation CA - T1 • VeriSign Class 3 Extended Validation SGC CA - T1 • Symantec Class 3 DSA EV SSL CA • Symantec Class 3 ECC 256 bit Extended Validation CA • Symantec Class 3 ECC 384 bit Extended Validation CA • Symantec Class 3 EV SSL CA - G2 • Symantec Class 3 EV SSL CA - G3 • Symantec Class 3 EV SSL SGC CA - G2 • Symantec Class 3 Extended Validation SHA256 SSL CA • Symantec Class 3 ECC 256 bit EV CA - G2 • Symantec Class 3 ECC 256 bit EV CA - G3 • Symantec Class 3 EV SSL CA - G4

Assertion of Management as to
Its Disclosure of its Business Practices and its Controls
Over its Extended Validation Certification Authority Operations
During the period from December 1, 2015 through June 15, 2016

February 28, 2017

Symantec Corporation ("Symantec") provides its Extended Validation SSL ("EV SSL") Certification Authority (CA) services through the Symantec Trust Network (STN) CAs listed in Appendix A ("the STN Root and EV SSL Issuing CAs").

The management of Symantec is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key life cycle management controls, and EV SSL certificate life cycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Symantec's certification authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Symantec management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in Symantec management's opinion, in providing its EV SSL Certification Authority (CA) services at Mountain View, California, USA; New Castle, Delaware, USA; Melbourne, Australia; Dublin, Ireland; and Kawasaki-shi, Japan, throughout the period December 1, 2015 to June 15, 2016, Symantec has:

- disclosed its extended validation SSL ("EV SSL") certificate life cycle management business practices in its Symantec Trust Network Certification Practice Statement, Version 3.8.24 dated May 20, 2016 ("STN CPS"); and Symantec Trust Network Certificate Policy, Version 2.8.20, dated May 20, 2016 ("STN CP") including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the Symantec website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their life cycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by Symantec)

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.4.5 except for the effects of the matters noted below.

Impacted WebTrust for CAs Criteria		Matters Noted
1	Verification of Applicant Principle 2, Criterion 13 requires that the CA maintains controls and procedures to provide reasonable assurance that for each Fully-Qualified Domain Name listed in a Certificate, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by only using at least one of the following verification methods: 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; 2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field; 4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at -sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; Verification of EV SSL Certificate requests Principle 2, Criterion 18 requires that in cases where an EV SSL Certificate Request is submitted by a Certificate Requester, the CA maintains controls to provide reasonable assurance that, before it issues the requested EV SSL Certificate, it verifies that an authorized Certificate Approver reviewed and approved the EV SSL Certificate Request.	It was noted that Issuing EV SSL CAs were used to issue certificates for Symantec internal testing purposes for registered domains that Symantec did not own. As required by the CPS, Symantec did not obtain the required authorization from the respective registered domain owners prior to certificate issuance. Furthermore, certificates were also issued for internal testing purposes to unregistered domains. As we disclosed in our published incident reports, Symantec has completed a thorough investigation of its test certificates. Symantec's investigation uncovered no evidence of malicious intent, nor inappropriate use of these certificates. Each of these test certificates was issued solely for internal Symantec testing purposes that have since been revoked or have expired. Symantec contacted the relevant domain owners and provided relevant information to the browser community to enable the browsers to evaluate the appropriateness of blacklisting these test certificates where they deemed appropriate. We have also disabled access to technical features that enabled mis-issuance of test certificates; we updated our policies, internal procedures and trainings to clarify the April 2014 change in the Baseline Requirements that removed authorization to issue certificates to unregistered domains; we updated our internal policies, procedures and trainings to strongly reinforce that test certificates must follow the same authentication procedures as commercial certificates; and we performed a system update to ensure those domains identified that were associated with mis-issuances cannot be used for new certificates without first undergoing standard authentication and issuance procedures.

Impacted WebTrust for CAs Criteria		Matters Noted
2	Principle 2, Criterion 49 requires that the CA and RA maintain controls to provide reasonable assurance that event logs at the CA and RA site are retained for at least seven years.	It was noted that physical access entry and exit logs for one of the CA facilities were not archived for a minimum of 7 years, as specified in the CPS, to meet Principle 2, Criterion 49. Access log retention requirements for Symantec CA facilities exceed Symantec Corporate Security requirements. Due to recent personnel changes within the Corporate team that manages data retention across the company, CA facility log retention periods were reduced to match Corporate security log retention requirements without approval from the Symantec Website Security business unit. Upon identification and communication of the issue, the retention periods of physical access logs have since been updated to comply with the respective requirements for CA facilities. In addition, policy updates have been put in place to require supplemental approval and periodic monitoring of data retention requirements moving forward.

Symantec Corporation

Roxane Divol
EVP and GM, Website Security